IBM Security

# IBM Security Strategy:

## Changing to a Risk Based Program and Creating Digital Trust: The Weather Company

Klint Borozan
klintb@ibm.com

Industry Leader Telco Media & Entertainment

NAB Conference 2019



IBM


# What is Digital Trust?

"…Digital Trust is the measure of customer, partner, and employee confidence levels in the organizations ability to protect users, data, applications, transactions, and devices…"

# What we're hearing from organizations…


From thousands of engagements across the world, we've heard most common security concerns…Telco's, Media, Global Enterprise, E&U, Airlines, Financial, etc.

## Help me get there…

Modernize security frameworks and controls

Respond to the global security skills shortage

Address increasing cyber attack vectors including IoT

Secure the journey to cloud and digital transformation

Maintain data privacy and regulatory compliance

# The 3 Important Conversations took place:

## Security Strategy & Risk Transformation

- The first conversation is around security transformation…i.e. Risk Management
- Vs. Compliance and ad hoc
- Usability and consumability associated with risk management controls
- Gaps limiting ability to move forward
- Getting more from what you have & building on it:
  - AI, Orchestration, Cloud, & Collaboration
  - How well tools align to threats

## How do you run your threat mgmt program?

- Detection
  - Looking at historical information i.e. Relevant Log Sources
  - Logs + Flow Data
  - User Behaviors + DPI
- Investigation
  - Automating away from manual Google searches
  - Log and Data enrichment
  - Role of Cognitive
  - Visualization of attack kill chain
- Mitigation
  - Areas of Ad hoc response
  - Automation based on policy

## Digital Trust

- Protection of 5 Categories: Users, Data, Applications, Transactions, & Devices
- Its not about the latest tool to meet the newest threat
- Its about creating a protection model using roughly 11 different risk management controls across the 5 Categories
- Roles, Policies, and Variance measurement
- It is also about Governance
- Making it actionable

# From experience we know…11 Different Risk Management Controls across 5 Key Categories…working together

| Users | Applications | Data | Transactions | Devices/Hosts |
|---|---|---|---|---|
| 1) Identity governance, discovery, role based access models, variance measurement | -Management of the development and deployment process for security and vulnerabilities | 7) Encryption at rest and in motion…knowledge that any file or information that leaves is encrypted | 10) Fraud Prevention | 11) Configuration and Management |
| 2) Access management | 5) Static | 8) Data & File Activity Monitoring….out of policy alerts…lock it down | -Role of AI and Machine Learning | – Protected |
| 3) Cloud identity management systems, provisioning/de-provisioning(insider) | 6) Dynamic | 9) Discovery & Classification of narrow areas of critical data: locate, identify, lock it down, & Visualize | -Active analytics | – Manageable |
| 4) Privilege | *(Secure deployment) | | -Continuous Identity | |

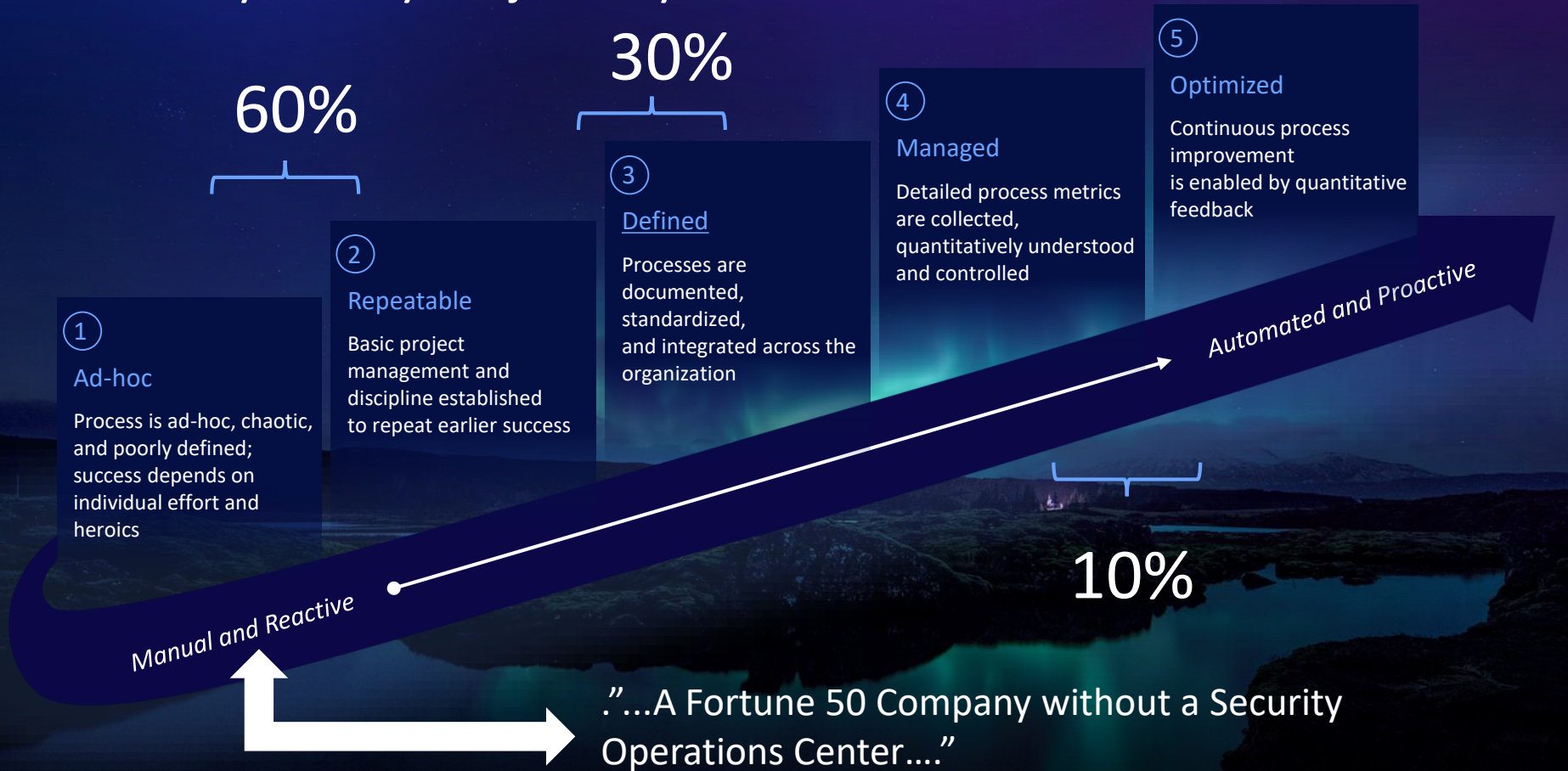
# Lets talk about how it applies to TWC…

- What are Media Companies? Content Developers, Cloud Video providers, Saas Provider, Cloud Services Consumers, Application Developers, Multi Cloud, etc.
- Under constant attack with attempts at critical data & content theft, data manipulation, DDoS, etc.
- Now a world class Security Operation
- Digital Trust

# Every organization is on a security continuum…


| What organizations tell us they need: | Guidance & Wisdom | Tools & Resources | Clarity & Action |
|---|---|---|---|
| Security needs to deliver: | Strategy, global visibility and industry expertise, an understanding of the value of time | Security controls working as one integrated risk management ecosystem | Empowered leadership + Tools: AI driven, prescriptive analytics and security orchestration |

# Where are you on your journey? TWC…




."...A Fortune 50 Company without a Security Operations Center…."

# Final Thoughts…

## Strategy and Risk

*Unify business leaders with security risk management*

## Threat Management

*Identify and respond to threats with speed and confidence*

## Governance & Leadership

*Measurement, Process, Policies, Involvement, Change Management*

## Digital Trust

*Govern and protect your business operations, data, users, partners, and assets*